Article

Chinese Science Bulletin

Communication

November 2013 Vol.58 No.31: 3859–3862
doi: 10.1007/s11434-013-6037-2

The security of decoy state protocol in the partial photon number splitting attack

LIU Dong, WANG Shuang*, YIN ZhenQiang, CHEN Wei & HAN ZhengFu

Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China

Received January 21, 2013; accepted April 22, 2013

The decoy state protocol was proposed to overcome the primitive photon number splitting attack. When using a better strategy, the attacker can ensure that the ratio of the overall gain of the signal state pulse against the decoy state pulse changes very little, even to keep the overall gain of the signal state pulses equal to that obtained without attacker. In this paper we first give a model of the partial photon number splitting attack which contains the original one, and then find that the decoy state protocol still works effectively under the partial photon number splitting attack.

photon number splitting attack, quantum key distribution, decoy state, overall gain, security

Citation: Liu D, Wang S, Yin Z Q, et al. The security of decoy state protocol in the partial photon number splitting attack. Chin Sci Bull, 2013, 58: 3859–3862, doi: 10.1007/s11434-013-6037-2

Quantum key distribution (QKD) makes two communication entities, Alice and Bob, sharing a secure random sequence. The most commonly used protocol, BB84 protocol, is based on the single photon source. But for the limitations of the technical, the actual QKD systems usually use the weak coherent source, where the statistical distribution of the number of photons is Poisson distribution. So the practical pulse sequence contains some multi-photon pulses, even when the average photon number of a pulse is about 0.1. The eavesdropper can use this weakness to do photon number splitting (PNS) attack [1–3]. Her attack strategy is to remove all the single photon pulses and steal one photon from each multi-photon pulses, and then send the rest to Bob over a lossless channel. Since the photons stolen by Eve carry the same information with photons sending to Bob, Eve can obtain all the information between the legitimate users.

Using the method of decoy state [4–6] is a very good solution to overcome the splitting attack. In the decoy state protocol, Alice and Bob use different intensity of the laser to confuse the attacker. Using the gain and the error rate of the signal sate and decoy state, legitimate users can calculate the lower bound of Q_1 and the upper bound of E_1. They are the response rate and quantum bit error rate (QBER) of the single photon pulses respectively. Then they can calculate the secure key rate by the GLLP formula [7,8],

$$R \geqslant q\{-Q_\mu f(E_\mu)H_2(E_\mu)+Q_1[1-H_2(E_1)]\}, \quad (1)$$

where, q is associated with the used protocol, for BB84 protocol q is set to 0.5. Q_μ and E_μ are measured directly from the experiment, they are the gain and the QBER of the signal pulses with the average photon number of μ. Function $f(x)$ indicates the error correction efficiency, and the function $H_2(x)$ indicates the binary Shannon information. In the past few years, many point-to-point QKD experiments and QKD networks based on the decoy state method have been proposed [9–16].

In PNS attack strategy, when the loss of the quantum channel between the two legitimate users is very large, the gain at Bob's side may be very large when Eve using the lossless channel. An improved strategy proposed by Chen et al. [17] is use to solve this problem. In this new strategy, attacker would need additional blocking part of the multi-photon pulses. On the contrary, when the loss of the quan-

*Corresponding author (email: wshuang@ustc.edu.cn)

tum channel is low enough, Eve can not compensate the yield of pulses. So in this case, she may use a new strategy that is letting some of the single photon pulses through. The partial photon number splitting attack contains those two strategies. Choosing appropriate passing fractions, Eve can ensure that the ratio of the overall gain of the signal state against the decoy state changes very little, even to ensure the overall gain of the signal state pulse equal to that obtained without attack. So under those attack strategies, the system based on BB84 protocol with decoy state method can generate the security key? In the rest of the paper we will give a model for the PNS attack which will contain the above attack strategies and then analyze the security of the decoy state protocol under this attack mode.

1 Model of the partial PNS attack

The actual system uses the attenuated laser pulses. The distribution of the photon numbers in each pulse is Poisson. For a one decoy system, Alice set the signal state and decoy state's average photon numbers to μ and v. The quantum channel's length is ℓ (km), with the loss coefficient α (dB/km). Then we can express the transmittance of the quantum channel as $\eta_\ell = 10^{-\alpha\ell/10}$. If there is no eavesdropper, the photon number distribution at Bob's side is still Poisson, with average photon number $\mu\eta_\ell$,

$$P_\ell[n] = \frac{(\eta_\ell \mu)^n}{n!} \mathrm{e}^{-\eta_\ell \mu}. \tag{2}$$

In the partial PNS attack, Eve's attack strategy is blocking part of single photon pulse and multi-photon pulse. The blocking ratios are $1-P_x$ and $1-P_y$. She extracts one photon from each pulse of the rest P_y multi-photon pulses, and then sends those pulses and the rest P_x single photon pulse to Bob. In this case, the photon number at Bob s side no longer follows Poisson distribution, but

$$P_{\mathrm{PNS}}[n] = \begin{cases} 1 - P_y + (P_y + P_y\mu - P_x\mu)\mathrm{e}^{-\mu} & n = 0, \\ \left(P_x\mu + P_y\dfrac{\mu^2}{2}\right)\mathrm{e}^{-\mu} & n = 1, \\ P_y\dfrac{\mu^{n+1}}{(n+1)!}\mathrm{e}^{-\mu} & n > 1. \end{cases} \tag{3}$$

This mode contains several PNS attack strategies. When $\{P_x=0, P_y=1\}$, it is just the primitive attack scenario, where Eve only deals with the multi-photon pulses. When the channel transmittance is very small, in order to reduce the probability of been discovered, Eve need to block some of the multi-photon pulse or use a loss channel, thus in this scenario $\{P_x=0, P_y\in(0.1)\}$. On the contrary, if the channel transmittance is very large, Eve may allow part of the single-photon pulses passing. Choosing an appropriate value of P_x and P_y, Eve may keep the ratio of the overall gain of the two states very close to that obtained without attack. Then the probability of discovery is maintained at a very low level.

2 The change of the overall gain

The transmittance of Bob's side is η_B, which includes the detector efficiency and the internal loss of the optical components. Y_0 is use to stand for the background noise, which includes the dark count of the detector and other noise. When there is no eavesdropper, Alice and Bob will find that the ratio of the overall gain between signal and decoy state is $\dfrac{Y_0 + 1 - \mathrm{e}^{-\eta\mu}}{Y_0 + 1 - \mathrm{e}^{-\eta\nu}}$, here $\eta = \eta_\ell\eta_B$.

When given a n-photon pulse at the entrance of the instrument of detection's side, the conditional response probability of the detector, Y_n, is given by

$$Y_n = Y_0 + 1 - (1-\eta_B)^n. \tag{4}$$

So under our PNS attack mode, the signal state's overall gain Q_μ at the detection's side can be expressed as

$$\begin{aligned} Q_\mu &= Y_0(1 - P_y + (P_y + P_y\mu - P_x\mu)\mathrm{e}^{-\mu}) + \\ &\quad Y_1\left(P_x\mu + P_y\frac{\mu^2}{2}\right)\mathrm{e}^{-\mu} + \sum_{n=2}^{\infty} P_y\frac{\mu^{n+1}}{(n+1)!}\mathrm{e}^{-\mu}Y_n \\ &= P_x\eta_B\mu\mathrm{e}^{-\mu} + P_y\left(1 - \mathrm{e}^{-\mu} - \frac{(\mathrm{e}^{-\eta_B\mu} - \mathrm{e}^{-\mu})}{(1-\eta_B)}\right) + Y_0. \end{aligned} \tag{5}$$

Similarly, the decoy state's overall gain Q_ν at the detection's side is

$$Q_\nu = P_x\eta_B\nu\mathrm{e}^{-\nu} + P_y\left(1 - \mathrm{e}^{-\nu} - \frac{(\mathrm{e}^{-\eta_B\nu} - \mathrm{e}^{-\nu})}{(1-\eta_B)}\right) + Y_0. \tag{6}$$

According to the decoy state method, if Alice or Bob find the ratio of the overall gain Q_μ/Q_ν much different from the ratio obtained without eavesdropper, they abort the whole protocol. Considering the vacuum + weak decoy state BB84 QKD system with GYS parameters [18], the mean photon number are set to $\mu = 0.6$ and $\nu = 0.2$, the quantum channel is 50 km with 0.21 dB/km loss coefficient, the whole transmittance at Bob's side is $\eta_B = 4.5\%$, and $Y_0 = 1.7\times10^{-6}$. So the overall gain of the signal state without eavesdropper is 0.0024 and the ratio of the overall gain is about 2.9934.

In the presence of Eve, we first consider that the overall gain of the signal state equal to that obtained without eavesdropper, then we can get the following condition equation,

$$P_x\eta_B\mu e^{-\mu}+P_y\left(1-e^{-\mu}-\frac{(e^{-\eta_B\mu}-e^{-\mu})}{(1-\eta_B)}\right)+Y_0$$
$$=Y_0+1-e^{-\eta_\ell\eta_B\mu}. \quad (7)$$

Using the above parameter values, this equation can be simplified to

$$\alpha P_x+\beta P_y=1-\gamma^{\eta_\ell}, \quad (8)$$

where $\alpha=\eta_B\mu e^{-\mu}$, $\beta=1-e^{-\mu}-(e^{-\eta_B\mu}-e^{-\mu})/(1-\eta_B)$ and $\gamma=e^{-\eta_B\mu}=0.9734$. From the simplified equation, the ratio of the through single-photon and multi-photon pulses P_x and P_y are related to the channel's transmission efficiency.

When the transmittance of the quantum channel is very low, Eve need to block part of the multi-photon pulses. Here, we get $\eta_\ell=0.0891$ when the quantum channel is 50 km. The ratio of the overall gain decreases as P_x increases and increases as P_y decreases. The results are shown in Figure 1. Eve selects the appropriate parameters to keep the overall gain of the signal states unchanged. When she set P_x to 0, she may obtain the most information of the key with a high probability to be discovered, since the ratio of the overall gain has value of 7.8562 which deviates obviously from 2.9934. And when she set P_y to 0, she can not get any information of the key. Only in the case she set P_x to 0.0906 and P_y to 0.1599, the ratio of the overall gain almost equal to the ratio obtained without eavesdropper, Eve may get part of information without been found.

In the normal case, she do not need the overall gain of the signal states remain the same with the value obtained without eavesdropper, the ratio of the overall gain changing with P_x and P_y are shown in Figure 2. Here P_x, $P_y\in[0,1]$. We find that when the ratio of P_x and P_y is about 0.57, selected an appropriate value of P_x, the value of Q_μ/Q_ν is almost close to the value got from the case without attack.

3 The security analysis

In partial PNS attack, Eve might steal some information

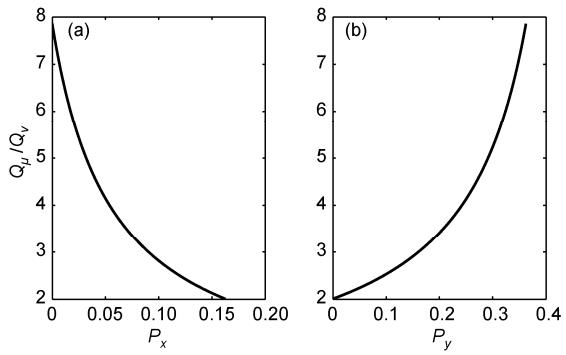

Figure 1 The ratio of the overall gain changed with P_x and P_y, respectively, when the overall gain of the signal states equal to that obtained without eavesdropper.

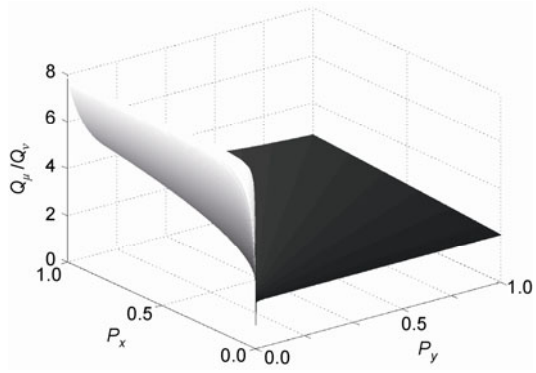

Figure 2 The ratio of the overall gain changed with P_x and P_y.

without been detected. However, Alice and Bob can remove the stolen information by post processing. Using the decoy state protocol, first we need to get the lower bound of the conditional probability of the detection event when given that Alice sends a single photon pulse, then we can estimate the QBER of single photon pulses E_1 and the gain of single photon pulses Q_1. This lower bound of the conditional probability can be calculated by

$$Y_{[1]}\geqslant Y_{[1]}^L=\frac{\mu}{\mu\nu-\nu^2}\left(Q_\nu e^{\nu}-Q_\mu\mu e^{\mu}\frac{\nu^2}{\mu^2}-\frac{\mu^2-\nu^2}{\mu^2}Y_0\right). \quad (9)$$

However, the actual value of this conditional probability under the partial PNS attack can be expressed as

$$Y_{[1]}^F=P_x\eta_B+Y_0. \quad (10)$$

According to the decoy state theory, if the actual value of the conditional probability is bigger than the lower bound, it means that the two legitimate users can always share the secure key.

In the case that the overall gain of the signal state pulses equal to that obtained without eavesdropper, for a given P_x, we can obtain the overall gain of the two states by the eqs. (5) and (6), and then compare the lower bound obtained by the eq. (9) with the actual value obtained by the eq. (10). The Figure 3 shows those two values. The solid line represents lower bound and the dotted line represents the actual value. The solid line is always below the dotted line, which means that $Y_{[1]}^F>Y_{[1]}^L$ is always true and Alice and Bob can always generate secure keys according to the GLLP formula. So the system with decoy protocol is safe in this special PNS attack.

In the normal case, Eve can randomly select the values of P_x and P_y. For a given P_x, we first get the maximum value of $Y_{[1]}^L$ for all P_y, then compare the actual value with this maximum value. The Figure 4 is given this result. The solid line represents the maximum value and the dotted line represents the actual value. The solid line is always below the dotted line, this means $Y_{[1]}^F>Y_{[1]}^L$ is always true. So the legitimate

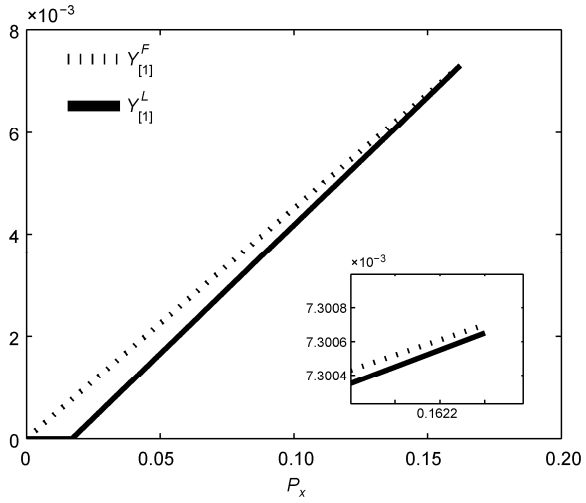

Figure 3 Condition: the overall gain of the signal state pulses equal to that obtained without eavesdropper. The solid line represent the value of the lower bound for a given P_x, the dotted line represent the actual value.

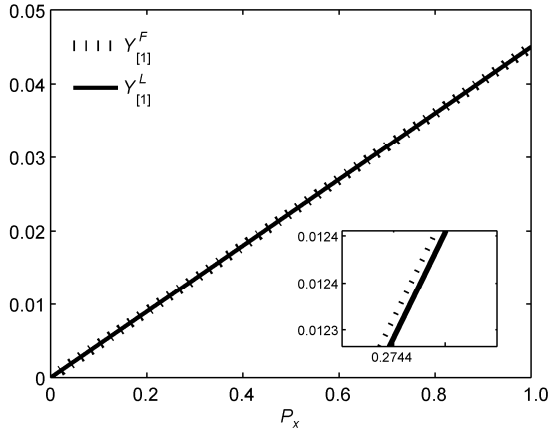

Figure 4 The solid line represent the value of the lower bound for a given P_x, the dotted line represent the actual value.

users can always generate secure key in the normal case. Thus we can conclude that the system with decoy protocol is safe in any type of PNS attack.

4 Conclusion

We gave a model of the partial PNS attack, in which the PNS attack is a special case. Then, based on the model, we analyzed the change of the overall gain and found that the ration of the overall gain of the signal-state pulses against that of the decoy-state pulses changed rapidly with the fractions of the pass single photon pulse and the multi-photon pulses. When choosing appropriate fraction, the ratio can remain unchanged which means that eavesdropper may obtain part of the key information with a lower probability to be discovered. Finally, we proved the decoy-state protocol is secure under the partial PNS attack.

This work was supported by the National Basic Research Program of China (2011CBA00200 and 2011CB921200), the National Natural Science Foundation of China (60921091 and 61101137), China Postdoctoral Science Foundation (2012M511419) and Technology projects funded of State Grid Corporation (XX17201200028).

1 Huttner B, Imoto N, Gisin N, et al. Quantum cryptography with coherent states. Phys Rev A, 1995, 51: 1863–1869
2 Lutkenhaus N. Security against individual attacks for realistic quantum key distribution. Phys Rev A, 2000, 61: 052304
3 Brassard G, Lutkenhaus N, Mor T, et al. Limitations on practical quantum cryptography. Phys Rev Lett, 2000, 85: 1330–1333
4 Hwang H K. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901
5 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503
6 Lo H K, Ma X F, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504
7 Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices. Quant Inform Comput, 2004, 5: 325–360
8 Ma X F, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution. Phys Rev A, 2005, 72: 012326
9 Yin Z Q, Han Z F, Chen W, et al. Experimental decoy state quantum key distribution over 120 km fiber. Chin Phys Lett, 2008, 25: 3547
10 Wang S, Zhang S L, Li H W, et al. Decoy-state theory for the heralded single-photon source with intensity fluctuations. Phys Rev A, 2009, 79: 062309
11 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chin Sci Bull, 2009, 54: 2991–2997
12 Hu J Z, Wang X B. Reexamination of the decoy-state quantum key distribution with an unstable source. Phys Rev A, 2010, 82: 012331
13 Wang S, Chen W, Yin Z Q, et al. Field test of wavelength-saving quantum key distribution network. Opt Lett, 2010, 35: 2454–2456
14 Liu D, Yin Z Q, Wang S, et al. Estimation of key rate after setting dead time. Chin Phys B, 2012, 21: 060202
15 Zhang L J, Wang Y G, Yin Z Q, et al. Real-time compensation of phase drift for phase-encoded quantum key distribution systems. Chin Sci Bull, 2011, 56: 2305–2311
16 Lutkenhaus N, Jahma M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. New J Phys, 2002, 4: 44
17 Chen H, Huang Y S, Liu Y M. Security analysis of decoy-state quantum key distribution system (in Chinese). Infor Sec Commu Pri, 2011, 8: 56–58
18 Gobby C, Yuan Z L, Shields A J. Quantum key distribution over 122 km of standard telecom fiber. Appl Phys Lett, 2004, 84: 3762–3764